Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for monitoring network packets transmitted within a distributed data processing system, the method comprising:

monitoring multiple sources of network packets within the distributed data processing system;

identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions by deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets, receiving packet filtering parameters at each of the deployed distributed packet snoopers, and matching packet filtering parameters against transmitted packets, wherein the packet filtering parameters specify at least a packet type and a packet size of a packet; and

alerting a system administrator to the identified source of network packets by returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters.

2. (Previously Presented) The method of claim 1 wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value.

3. (Previously Presented) The method of claim 1 wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size.

4. (Previously Presented) The method of claim 1 wherein a predetermined condition of the one or more predetermined conditions is a count of a number of packets, where the number of

packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, that exceed a predetermined maximum count threshold value.

5. (Previously Presented) The method of claim 1 wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, in comparison to a number of packets from the identified source of network packets.

6. (Original) The method of claim 1 further comprising:

in response to a request of the system administrator, halting execution of the identified source.

7. (Original) The method of claim 1 further comprising:

in response to a request of the system administrator, pausing execution of the identified source.

8. (Original) The method of claim 1 further comprising:

initiating a packet snooping session.

9.-10. (Cancelled)

11. (Currently Amended) The method of claim [[10]] 1 further comprising:

receiving a request for an action at a target resource within the distributed data processing system, wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application.

12. (Original) The method of claim 11 further comprising:

deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource.

13. (Original) The method of claim 11 further comprising:

selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system.

14. (Original) The method of claim 11 further comprising:

deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action.

15. (Original) The method of claim 1 further comprising:

displaying the identified source of network packets to the system administrator in real time.

16. (Currently Amended) An apparatus for monitoring network packets transmitted within a distributed data processing system, the apparatus comprising:

means for monitoring multiple sources of network packets within the distributed data processing system;

means for identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions; and

means for alerting a system administrator to the identified source of network packets by returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters, wherein the means for identifying comprises:

means for deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets;

means for receiving packet filtering parameters at each of the deployed distributed packet snoopers, wherein the packet filtering parameters specify at least a packet type and a packet size of a packet; and

means for matching packet filtering parameters against transmitted packets.

17. (Previously Presented) The apparatus of claim 16 wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value.

18. (Previously Presented) The apparatus of claim 16 wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size.

19. (Previously Presented) The apparatus of claim 16 wherein a predetermined condition of the one or more predetermined conditions is a count of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, that exceed a predetermined maximum count threshold value.

20. (Previously Presented) The apparatus of claim 16 wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, in comparison to a number of packets from the identified source of network packets.

21. (Original) The apparatus of claim 16 further comprising:

means for halting execution of the identified source in response to a request of the system administrator.

22. (Original) The apparatus of claim 16 further comprising:

means for pausing execution of the identified source in response to a request of the system administrator.

23. (Original) The apparatus of claim 16 further comprising: means for initiating a packet snooping session.

24.-25. (Cancelled)

26. (Currently Amended) The apparatus of claim [[25]] 16 further comprising:

means for receiving a request for an action at a target resource within the distributed data processing system, wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application.

27. (Original) The apparatus of claim 26 further comprising:

means for deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource.

28. (Original) The apparatus of claim 26 further comprising:

means for selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system.

29. (Original) The apparatus of claim 26 further comprising:

means for deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action.

30. (Original) The apparatus of claim 16 further comprising:

means for displaying the identified source of network packets to the system administrator in real time.

31. (Currently Amended) A computer program product in a computer-readable medium for use within a distributed data processing system for monitoring network packets transmitted within the distributed data processing system, the computer program product comprising:

instructions for monitoring multiple sources of network packets within the distributed data processing system;

instructions for identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions; and

instructions for alerting a system administrator to the identified source of network packets by returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters, wherein the instructions for identifying comprises:

instructions for deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets;

instructions for receiving packet filtering parameters at each of the deployed distributed packet snoopers, wherein the packet filtering parameters specify at least a packet type and a packet size of a packet;

instructions for matching packet filtering parameters against transmitted packets.

32. (Previously Presented) The computer program product of claim 31 wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value.

33. (Previously Presented) The computer program product of claim 31 wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size.

34. (Previously Presented) The computer program product of claim 31 wherein a predetermined condition of the one or more predetermined conditions is a count of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, that exceed a predetermined maximum count threshold value.

35. (Previously Presented) The computer program product of claim 31 wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, in comparison to a number of packets from the identified source of network packets.

36. (Original) The computer program product of claim 31 further comprising:

instructions for halting execution of the identified source in response to a request of the system administrator.

37. (Original) The computer program product of claim 31 further comprising:

instructions for pausing execution of the identified source in response to a request of the system administrator.

38. (Original) The computer program product of claim 31 further comprising:

instructions for initiating a packet snooping session.

39.-40. (Cancelled)

41. (Currently Amended) The computer program product of claim [[40]] 31 further comprising:

instructions for receiving a request for an action at a target resource within the distributed data processing system, wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application.

42. (Original) The computer program product of claim 41 further comprising:

instructions for deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource

43. (Original) The computer program product of claim 41 further comprising:

instructions for selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system.

44. (Original) The computer program product of claim 41 further comprising:

instructions for deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action.

45. (Original) The computer program product of claim 41 further comprising:

instructions for displaying the identified source of network packets to the system administrator in real time.